



Santa Clara High Technology Law Journal

Volume 19 | Issue 1

Article 3

January 2003

Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce

Pablo Baistrocchi

Follow this and additional works at: <http://digitalcommons.law.scu.edu/chtlj>



Part of the [Law Commons](http://digitalcommons.law.scu.edu/chtlj)

Recommended Citation

Pablo Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, 19 SANTA CLARA HIGH TECH. L.J. 111 (2002).

Available at: <http://digitalcommons.law.scu.edu/chtlj/vol19/iss1/3>

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.

LIABILITY OF INTERMEDIARY SERVICE PROVIDERS IN THE EU DIRECTIVE ON ELECTRONIC COMMERCE

Pablo Asbo Baistrocchi†

I. INTRODUCTION

The growth of e-commerce has been extremely rapid in recent years. By the year 2000, its worth exceeded 17 billion euro, and it is expected to reach 340 billion euro by the end of 2003.¹ These numbers reflect the importance of this factor in the construction of the internal European market. In striving for the high level of harmonization necessary for the many issues related to this industry, it is important that there be due regard for the predictable downstream effects and a method of systematic prioritization.

This Article will deal with a key element in the development of e-commerce initiatives within the European Union: the liability of intermediary service providers [hereinafter ISPs]. The structure of the Article will begin with a discussion of the main aims of the EU Directive dealing with these important concepts; followed by an examination of the different levels of liability to which ISPs are exposed, the areas of liability that can be touched through ISP activities, and the diverse roles that ISPs play. Next, in describing the formulations surrounding the issue, the liability of ISPs within the activities covered by the Directive will be discussed. And finally,

† Pablo Asbo Baistrocchi holds a *Joint Master in European Law* (LLM) from Maastricht University (The Netherlands) and the University of Nottingham (UK). He has also been awarded a *Certificate in European Law* from the European University Institute in Florence, Italy. He received his first degree in law from the Catholic University of Uruguay in Montevideo. He has been one of the European Union Editors of *Europemedia*, an Internet research company based in Amsterdam. He is currently working at the European Commission in the Information Society Directorate General. All the opinions expressed in the Article are solely of the author and do not engage any organization where he is or was professionally linked.

1. See European Commission, *Electronic Commerce: Commission Welcomes Final Adoption of Legal Framework Directive*, available at http://europa.eu.int/comm/internal_market/en/ecommerce/2k-442.htm (summarizing the Council Directive 2000/31 of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market).

some recommendations to improve the Directive's effectiveness in the context of the Digital Millennium Copyright Act² [hereinafter DMCA] of the United States will be discussed, as the current EU Directive draws many of its provision from the DMCA.

II. AIMS OF THE DIRECTIVE ON E-COMMERCE

The motivation behind the EU Directive on electronic commerce is to develop information society services [hereinafter ISS], ensure legal certainty and consumer confidence through the coordination of national laws, and clarify legal concepts for the proper functioning of the internal market, in order to create a legal framework to ensure the free movement of ISS between Member States.³ This specific "free movement of services" is part of a general principle of law in the European Economic Community [hereinafter Community], namely freedom of expression, as enshrined in Article 10(1) of the European Convention on Human Rights and Fundamental Freedoms.⁴ This principle is subject only to restrictions expressed in paragraph 2 of that Article and in Article 56 (1) of the EC Treaty.⁵

Specifically, the Directive's aims regarding liability issues are to streamline the functioning of the internal market, enhance the development of cross-border services, and eliminate distortions of competition through the harmonization of national provisions concerning liability of ISPs acting as intermediaries.⁶ The Directive also intends to be the appropriate foundation for the establishment, through voluntary agreements between all parties concerned and encouraged by Member States, of reliable procedures for removing and disabling access to illegal information.⁷

2. Digital Millennium Copyright Act, § 202, Pub. L. No. 105-304, 112 Stat. 2860, 17 U.S.C. § 512 (1998).

3. See Council Directive 2000/31, 2000 O.J. (L 178) 3, recital 5-7, available at <http://europa.eu.int> (discussing certain legal aspects of information society services, in particular electronic commerce in the internal market) [hereinafter Directive].

4. Convention for the Protection of Human Rights and Fundamental Freedoms, Dec. 10, 1948, art. 10(1), EUR. CONSULT. ASS., Europe. T.S. No. 005. "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises." *Id.* [hereinafter Convention].

5. Treaty Establishing The European Economic Community, Mar. 25, 1953, art. 56(1), 298 U.N.T.S. 3 (1953) [hereinafter EC Treaty]. "The provisions of this Chapter and measures taken in pursuance thereof shall not prejudice the applicability of provisions laid down by law, regulation or administrative action providing for special treatment for foreign nationals on grounds of public policy, public security or public health." *Id.*

6. Directive, *supra* note 3, at recital 40.

7. *Id.* at recital 40.

III. IMPORTANT CONCEPTS

Before getting into an analysis of the Directive's provisions regarding ISP liability, it is appropriate to define the concepts for the different terms that will be dealt with throughout the remainder of this Article.

First, the Directive defines "information society services" as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service."⁸ Some of the activities included in the definition are the sale of goods on-line, the transmission of information via a communication network, the hosting of information provided by a recipient of the service, services which are transmitted point to point, e.g., video-on-demand and commercial communications by electronic mail, and services which are not remunerated by those who receive them, e.g., tools allowing for search, access, and retrieval of data.⁹

The following terms are defined in Article 2: a "service provider" is "any natural or legal person providing an information society service," and an *established* service provider is a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period.¹⁰ The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider.¹¹ The "recipient" of the service is "any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible."¹² The "consumer" is "any natural person who is acting for purposes which are outside his or her trade, business or profession."¹³ And finally, within the coordinated field falls the requirements with which the service provider has to comply in respect of *inter alia*: the pursuit of its activity, such as requirements concerning its behavior, and requirements concerning its liability.¹⁴

8. *Id.* at recitals 17–18.

9. *Id.*

10. *Id.* at art. 2(a)–(c) (emphasis added).

11. *Id.* at art. 2(c).

12. Council Directive 2000/31, 2000 O.J. (L 178) 3, art. 2(d).

13. *Id.* at art. 2(e).

14. *Id.* at art. 2(n).

IV. TYPES OF LIABILITY

In determining when an ISP can be held liable, the determination of the type of liability that is applicable allows us to know whether the ISP will have to bear the weighty burden of a *strict* liability system, or a lighter *with-fault* liability system.

With a strict liability system, an ISP will be held liable regardless of its knowledge and control over the material that is disseminated through its facilities.¹⁵ This system is the most restrictive because an ISP can be stated as being responsible (and consequently liable) even though it does not have any knowledge or control over certain material. This system can be indirectly established through imposing an obligation to monitor all the material that is posted on the Internet.¹⁶ To comply with this obligation is a complex, technical task and often prohibitive from an economic point of view. The majority of small ISPs, who do not have all the means to fulfill a requirement like this, would face an enormous threat of potential liability.¹⁷

In a system based on fault, an ISP would be held responsible if it intentionally violates the rights of others.¹⁸ There are two distinct levels in this system: actual knowledge and constructive knowledge. Under *actual* knowledge, if the ISP knows that there is some material on the Internet that violates someone's rights, then the ISP will be held liable. Under the second level of *constructive knowledge*, the law may determine if the ISP has certain clues, or should have reasonably presumed that certain material was infringing someone's rights, thereby making the ISP liable.¹⁹ As will be discussed later, the liability system imposed by the Directive is closer to the latter, a with-fault system with a "constructive knowledge" requirement.

V. AREAS OF POTENTIAL LIABILITY

A number of legal problems arise regarding liability through the Internet, due in part to the relative ease in which individuals can perform various activities through the Internet. With little technical knowledge and no money,²⁰ any person in any part of the world can

15. Rosa Julia-Barcelo, *Liability for Online Intermediaries: A European Perspective*, CENTRE DE RECHERCHES INFORMATIQUE ET DROIT, at http://www.eclip.org/eclip_1.htm, 7, 10.

16. *Id.* at 10.

17. *Id.* at 23.

18. *Id.* at 7.

19. *Id.* at 7.

20. With a basic knowledge on surfing the Internet it is possible to set up a web page in a matter of minutes (and often at no subscription cost) through an increasing number of Internet

transmit, reproduce, or disseminate huge amounts of material of every type. Texts, pictures, songs, and movies can be posted on a Web site, using any of the tools commonly available through modern commercial technology. The problem is, therefore, not the posting of material itself, which cannot be controlled, but the content of the posted material, which can be illegal, harmful, obscene, or otherwise undesirable.

As such, various types of legal violations can occur through the use of on-line facilities the following when materials are displayed:

- *Copyright material.* Creative rights are one of the most affected areas of the law since with the Internet it is extremely easy to disseminate copyrighted work. It occurs when any kind of protected material (text, picture, music) is posted on a Web page without respecting the copyright holder's rights.
- *Illegal and harmful content.* This category includes material that can be labeled as pornographic, racist, or terrorist.
- *Private and defamatory material.* This kind of material includes pictures taken in intimate situations, information concerning the family situation, financial or tax statements, or otherwise private or derogatory material infringing various rights of privacy, including those contained in European data protection and anti-defamation laws.
- *Misrepresentation.* This may happen when false or incorrect information, provided by and disseminated using on-line facilities, causes damage to a third party.
- *Others:* this includes the infringement of other substantive laws such as patents, trademarks, and unfair trade practices.²¹

hosts. See e.g., Yahoo Geocities, at <http://geocities.yahoo.com/>.

21. Julia-Barcelo, *supra* note 15, at 6.

VI. ON-LINE INTERMEDIARIES ROLES

There are numerous players acting in the Internet world; some are totally separate commercial entities, and some are part of the same corporations. One of the most known is America On-Line (AOL),²² which plays several roles, such as access provider, host service provider, information location tool provider, and even content provider. The different roles played by the on-line intermediaries may affect the liability regime applicable.

Thus, focusing attention on the different roles that the on-line intermediaries play within cyberspace, the following entities can be described:

- Network operator: providing the technical facilities for the transmission of information.
- Access provider: providing users with access to the Internet.
- Search Engines: on-line tools used for finding Web sites such as Yahoo!, AltaVista, Google, etc. There are two types of search engines, namely, "automated" search engines and search engines that rely upon people to review and catalogue Web sites.
- Host service provider: services in which users may rent Web site space, set up Web pages, and upload content, such as software, text, graphics, or sounds. Hosting services may include on-line exchanges also, like bulletin boards and chat rooms.²³

Bulletin board and news group users can read information sent by other users and post their own messages. Usually, bulletin boards, news groups, and chat rooms are devoted to specific topics.²⁴ Chat rooms allow users to exchange files and communicate in real time

22. AOL is the leading internet access provider in the U.S. and the only provider with a pan-European presence. In Europe AOL operates mainly through two joint ventures: AOL Europe, a 50/50 deal with Bertelsmann, and AOL CompuServe France, a venture with both Bertelsmann and Vivendi subsidiaries Cegetel, and Canal Plus. See AOL Time Warner, Corporate Information, at http://www.aoltimewarner.com/corporate_information/index.adp.

23. Julia-Barcelo, *supra* note 19, at 3–4.

24. *Id.* at 4.

with each other. It is a more interactive service that also allows for files exchange.²⁵

VII. LIABILITY OF INTERMEDIARY SERVICE PROVIDERS

A. Preliminary Concepts

There are two approaches to deal with the liability of an ISP. In a *vertical* approach, different liability regimes apply to different areas of the law.²⁶ This is the approach adopted by the United States. The Digital Millennium Copyright Act²⁷ deals with copyright issues, whereas the Telecommunications Act of 1996²⁸ deals with liability derived from violations of other types of laws.²⁹ In a *horizontal* approach, there is one liability regime applicable to any infringement regardless of the area of law. Thus, the same regime will be applicable to any type of infringement, whether it is copyright, defamation, or privacy rights.³⁰ The horizontal approach is used by the EU Directive. It is argued, that a horizontal approach is favorable because ISPs do not have to monitor the content of the material published by their customers.³¹ If the EU had adopted a vertical approach that applied different legal liability regimes to the data flowing through the systems, ISPs would have been obliged to decode the bits that form the data and analyze all the content (music, images, etc) before posting. This would have been an extremely weighty burden to place on the ISPs' shoulders, with the possibility of converting them in censorship agents.³²

The Directive does not establish a general liability regime applicable to ISPs. Instead, it provides for a system of specific liability exemptions.³³ This means that in cases where the ISPs provide a specific service (mere conduit, caching, and hosting) and

25. It is much more difficult to detect copyright infringement in files exchanged in a chatroom than, for example, on a web page that displays a permanent link to static files.

26. Julia-Barcelo, *supra* note 19, at 15.

27. See DMCA, *supra* note 2, Julia-Barcelo, *supra* note 15, at 16.

28. Telecommunications Act of 1996, Pub. L. No. 104-104, Title V, 110 Stat. 56, 133-43 (1996).

29. The liability provisions of Title V of the DMCA remain valid and enforceable, though other sections have been struck down as unconstitutional. See Rosa Julia-Barcelo, *On Line Intermediary Liability Issues: Comparing EU and US Legal Frameworks*, 22 EUR. INTELLECTUAL PROP. REV. 105, 108 n.26 (2000).

30. Julia-Barcelo, *supra* note 19, at 15

31. *Id.*

32. *Id.* at 8.

33. *Id.* at 16, n. 27, Directive, *supra* note 3, at recital 45.

comply with a series of requirements, they will not be held liable for the services performed (within some limitations). The limitations apply only to liability for damages because the last paragraphs of Articles 12, 13, and 14 of the Directive establish that Member States retain the right to require the ISPs to terminate or prevent known infringements.³⁴ Moreover, it is stated in Recital 45 of the Preamble that the limits on the liability of ISPs includes injunctions of different types and court orders that require the “termination” or “prevention” of any infringement.³⁵ This includes prohibitory injunctions, where the ISPs are required to desist from wrongful activity, and mandatory injunctions, where ISPs are required to rectify any wrongdoing.

It must also be kept in mind that the Directive only provides for a system of liability exemptions for ISPs. Thus, if an ISP does not qualify for an exemption under the Directive, its liability will be determined by the national laws of the respective Member States.³⁶ Additionally, even when it is known that ISPs can undertake different activities, the Directive liability distinctions are based on different categories of services provided by the ISPs; rather than on different categories of services providers.

B. Activities of the ISP Covered by the Directive

It is important to emphasize that all on-line activities must be in contact with at least one ISP; therefore, it is important to have a clear way to avoid uncertainty when dealing with ISPs. There are different ways to accomplish this.³⁷ One way is to set up an objective exemption for specific activities. An objective exemption could provide freedom from liability for ISPs engaged in activities predetermined by the legislature as permissible. The Directive provides an objective exemption for ISPs engaged in “mere conduit” activities, as long as they have complied with the Article 12 requirements.³⁸ For “caching” and “hosting” services, the Directive provides subjective exemptions.³⁹ The applicability of subjective exemptions rests upon whether the ISP, in addition to complying with the objective criteria from Article 12, has complied with additional due diligence requirements.

34. See Directive, *supra* note 3.

35. *Id.* at recital 45.

36. Julia-Barcelo, *supra* note 19, at 8.

37. MIGUEL P. POCH, MENSAJES Y MENSAJEROS EN INTERNET: LA RESPONSABILIDAD CIVIL DE LOS PROVEEDORES DE SERVICIOS INTERMEDIARIES (Universitat Oberta de Catalunya, Mar. 2001), available at http://uoc.terra.es/art/uoc/0103008/peguera_imp.html.

38. See Directive, *supra* note 3, at art. 12.

39. *Id.* at art. 13–14.

1. Mere Conduit

Article 12 provides for two types of “mere conduit” activities. The first consists of “the transmission in a communication network of information provided by a recipient of the service.”⁴⁰ The ISP is playing a passive role in such activities by acting as a mere “carrier” of data provided by third parties through its network. The second type of mere conduit activity is commonly known as “providing Internet access.”⁴¹ Mere conduit activities include the automatic, intermediate and transient storage of the information transmitted, in so far as it takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.⁴²

This provision describes the process of “packet switching transmission,” which allows ISPs to store information for a shorter period of time in small pieces. The packet switching transmission process allows ISPs to provide mere conduit activities by making copies of the information for the sole purpose of carrying out the transmission of the information, without making the information available to subsequent users. The term “automatic” refers to the fact that the act of storage occurs through the ordinary operation of the technology. As interpreted by the government of the United Kingdom, the term “intermediate” means that the “storage of information is made in the course of the transmission,” and the term “transient” refers to the fact that “the storage of the information is temporary and not to be stored beyond the time that is reasonably necessary for the transmission.”⁴³

When ISPs meet the conditions established in Article 12, their standard of liability is “no liability.” This is because they have no control over the data flowing through their network. The ISPs cannot be held liable for the information transmitted as long as they do not perform the following steps:

- Initiate the transmission; i.e. the provider does not make the decision to carry out the transmission. The fact that a provider automatically initiates a transmission at the request of a recipient of its service does not mean that the

40. *Id.* at art. 12(1).

41. *Id.*

42. *Id.* at art. 12(1).

43. U.K. DEPARTMENT OF TRADE AND INDUSTRY, E-COMMERCE-THE ELECTRONIC COMMERCE DIRECTIVE (00/31/EC), ch. 6, at

http://www.dti.gov.uk/cii/e-commerce/europeanpolicy/e-commerce_directive_chapter6.shtml.

service provider initiated the transmission.⁴⁴

- Select the receiver of the transmission; applicable when the ISP selects receivers as an automatic response to the request of the user initiating the transmission. This includes forwarding e-mail to a mailing list, at the request of the recipient.⁴⁵
- Select or modify the information contained in the transmission; not including manipulations of a technical nature which take place in the course of the transmission, since such manipulations do not alter the integrity of the information contained in the transmission.⁴⁶

2. Caching

The purpose of a caching service is to avoid saturating the Internet with the repetitive high demand of certain material. ISPs decrease this demand-overload by locating the high demand data on remote servers, then storing copies of the material on local servers. This allows delivery to information seekers in the quickest way, because the data has less distance to travel to reach end-users. This automatic, intermediate, and temporary storage of data in local servers is called “caching” for the purposes of the Directive. Other types of caching, such as long-term caching,⁴⁷ are not included in the Directive and therefore are not included in the liability exemptions.

ISPs cannot be held liable when they perform caching on the condition that:

- The provider does not modify the information;⁴⁸

This is the basic condition to be held not liable. The rationale behind the exemptions is namely that the ISPs respect the content that their clients post on the Web in its entirety. Otherwise, the ISPs could be held liable, even when they did not create the information.

- The provider complies with conditions on access to the

44. Directive, *supra* note 3, at art. 12(1)(a)., Marie Potel, *A Review of Directive 2000/31 EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce*, in JEAN MONNET PAPERS ON THE EUROPEAN INFORMATION SOCIETY 32, at <http://www.rechten.rug.nl/eur/EISMonnetChair/Papers/Public/UT-paper.ps.pdf>.

45. Directive, *supra* note 3, at art. 12(1)(b).

46. Directive, *supra* note 3, at recital 12(1)(c).

47. For instance, mirror caching, which includes storage of entire web pages is not included because is neither automatic nor intermediate. See Poch, *supra* note 37, at 11.

48. Directive, *supra* note 3, at recital 43.

information;⁴⁹

This means that the conditions on access to the original data should be respected for the cached copies as well. Sometimes, the original party posting the information applies certain conditions to access; for example, a subscription fee for entering specific data. Accordingly, when the provider accesses the information for caching purposes, it must comply with the access requirements in place (plus, the following conditions), in order to avoid liability.⁵⁰

- The provider must comply with rules regarding the updating of information, specified in a manner widely recognized and used by industry;⁵¹
- The professional codes that deal with the update of the information must be used by the providers. This is important especially when the information that is cached is otherwise updated frequently, as in the case of personal information or scientific or economic information that must be very precise;⁵²
- The provider must not interfere with the lawful use of technology that is widely recognized and used by industry to obtain data on the use of the information;⁵³ and
- The provider must act expeditiously to remove or to disable access to the information it has stored upon obtaining *actual knowledge* of the fact that the information at the initial source of the transmission has been removed from the network, access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.⁵⁴

There are several situations under this last sub-requirement in which the provider cannot be held liable:

- The provider must allow the original Web owner or

49. *Id.* at recital 46.

50. *Id.* at art. 13(1)(b).

51. *Id.* at art. 13(1)(c).

52. *Id.*

53. *Id.* at art. 13(1)(d).

54. Directive, *supra* note 3, at art. 13(1)(e).

creator to get the information regarding the Web page access, i.e. from where and from whom the hits to his Web page come (that in this case will be to the cache copy instead of the original Web page).

- The provider generally acts expeditiously to remove or disable access to information it has stored, upon obtaining *actual knowledge* that at the initial source has been:
 - 1) removed from the network;
 - 2) access to the information has been disabled; or
 - 3) a competent authority has ordered the removal or disablement of the information.⁵⁵

Receipt of actual knowledge can often occur through a simple process. To begin with, it is important to keep in mind that Article 15 prohibits Member States from compelling ISPs to monitor the information which they transmit or store.⁵⁶ Thereby, the actual knowledge requirement must be interpreted in light of Article 15. That is to say, ISPs obtain actual knowledge if they receive the information from a third party, but not from their own inquiry upon the content of the information stored.⁵⁷ After having received the information concerning the three conditions of the original Web page, the ISPs must act promptly to remove the materials from its network.⁵⁸

3. Hosting

One key to success for the Internet is the opportunity for any individual to rent space from a host provide, where that individual may post any kind of material, at any time and at a very low cost—sometimes even for free. This rent can also be provided through bulletin boards and chat rooms. “Hosting,” therefore, defines the service that provides offers to individuals, companies, and organizations to rent space and incorporate any kind of data on the space.⁵⁹

ISPs will not be held liable for performing this activity as long

55. See generally Directive, *supra* note 3, at art. 13.

56. *Id.* at art. 15.

57. Julia-Barcelo, *supra* note 19, at 21.

58. *Id.*

59. Rosa Julia-Barcelo, *On Line Intermediary Liability Issues: Comparing EU and US Legal Frameworks*, 22 EUR. INTELLECTUAL PROP. REV. 105, 111 (2000).

as,

- the provider does not have actual knowledge of illegal activity or information and, as regarding claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.⁶⁰

It is also provided that the abovementioned shall not apply when the customer of the service is acting under the authority or the control of the provider.⁶¹ This reinforces the *raison d'être* behind the limitation of liability, namely that ISPs may be held liable if they have some form of “control” over the information.

Thus, mere knowledge or awareness of illegal activity alone is not enough alone to make a host provider liable, especially if the ISP acts promptly to remove the information or to disable access to it. Now, the problem of determining the precise meaning of actual knowledge reemerges.⁶² The Directive does not establish a “notice and take down” regime, as is found in the Digital Millennium Copyright Act⁶³ (DMCA) in the U.S. The following elements are part of the regime under the DMCA:

- The online service provider [hereinafter OSP] must have a designated agent to receive notices and it must use a public portion of its Web site for receipt of notices;
- The OSP must notify the U.S. Copyright Office of the agent’s identity and the Copyright Office will also maintain electronic and hard copy registries of Web site agents.⁶⁴

Proper written notification from a copyright owner to an OSP must include:

60. *Id.*

61. *Id.* at art. 14(2).

62. *See* Directive, *supra* note 3, recital 43, at 6.

63. *Compare* DMCA, *supra* note 2, at § (g)(2), with Directive, *supra* note 3.

64. *Id.* at § (c)(2).

- the name, address and electronic signature of the complaining party,
- sufficient information to identify the copyrighted work or works,
- the infringing matter and its Internet location,
- a statement by the owner that it has a good faith belief that there is no legal basis for the use of the materials complained of, and
- a statement of the accuracy of the notice and, under penalty of perjury, that the complaining party is authorized to act on behalf of the owner.⁶⁵

The only analogous provisions appearing in the Directive are found in Articles 14.3 and 21.2. Article 14.3 leaves Member States with the discretion to establish "notice and take down" procedure; and Article 21.2 provides that, when the Directive is next re-examined, the issues to be analyzed will include the notice and take down procedures and the attribution of liability following the taking down of content.⁶⁶

This *lacunae* in the Directive poses several problems. First and foremost is that ISPs would not be able to know whether they are properly informed, whether the information received is founded or not and whether they can face liability claims for Web page creators when their pages have been shut down.⁶⁷ This is especially the case if it has been proven that the content was neither illegal nor harmful. Consequently, a clear and detailed mechanism should be established that balances the competing interests at stake.

Whereas copyright holders have the right to protect their materials, Web creators have the right to express freely without a

65. *Id.* at §§ (c)(2)(A), (c)(3)(A).

66. It can be argued that a self-regulatory solution is envisaged in this regard, as flows from Article 16 of the Directive, which establishes that "Member States and the Commission shall encourage: (a) the drawing-up of codes of conduct at Community level, by trade, professional and consumer associations or organizations, designed to contribute to the proper implementation of Articles 5 to 15." See Directive, *supra* note 3, at art. 16.1(a). Based on Articles 14.3 and 16 *lit.a*, it can be inferred that Member States can either enact by itself or prompt professional organizations to enact codes of conduct which include notices and takes down procedures.

67. In this regard, the DMCA provides that "a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringed." DMCA, *supra* note 2, at § (g)(1).

permanent threat of being removed or disabled after an unfounded complaint has been received by the host provider, and the host providers have the right to have predetermined guidelines that allow them to know whether to disable access to a Web page or not.⁶⁸ Even if tough specific requirements for the notices of copyright infringements are established, the risk of an unfounded claim cannot be totally ruled out. It is therefore necessary to set up the so-called "put back procedure."⁶⁹ It is possible through such a procedure to obtain more complete protection for all the actors involved, as well as a proper balance between freedom of expression and fair competition. Through this mechanism, a person whose Web page has been disabled has the right to request its replacement or re-posting. If this request is made in compliance with the guidelines, then the host provider has to restore access to the Web page.⁷⁰ If a court action is then filed for the removal of access to the material from the host provider site, the ISP must do so. It has been submitted however, that within the European framework it would be better to decide that an ISP should disable access only if a court injunction is issued.⁷¹

Finally, it is worth considering what type of liability is imposed upon the sender of unfounded notices to ISPs which lead to the removal of material. Under the DMCA liability is imposed to the person who sends an intentional false notification.⁷² There is no provision concerning this issue in the E-commerce Directive. As a result, national liability laws will apply. And because in most of these laws liability is based on fault,⁷³ only when national courts finds that the sender was aware of the lack of proper grounds to send the notice

68. ESPRIT PROJECT 27028, *Electronic Commerce Legal Issues Platform, Recommendations to the Commission, Liability of Online Intermediaries*, available at http://europa.eu.int/ISPO/legal/en/lab/991216/recomm_liability.pdf.

69. *Id.*

70. *Id.*

71. *Id.*

72. DMCA, *supra* note 2, at § (c)(3)(B)(ii).

73. *E.g.*, in France, the CODE CIVILE states that "anyone who, through his act causes damage to another by his fault shall be obliged to compensate the damage." CODE CIV. art. 1382 (Fr.) translated in Code Napoleon 373 (1841). The German BGB provides that recovery for injury will be available if it was caused "willfully or negligently." See BÜRGERLICHES GESETZBUCH art. 823 (F.R.G.) translated in GERMAN CIVIL CODE 153 (1994). The Nordic countries that belong to the EU base tort law on a wrongdoer's liability for his or her own actions. The Dutch Civil Code, for instance, requires that an unlawful act be attributable to the tortfeasor's willful actions before it may be imputed to him or her; or that it be a cause of an injury for which he or she is accountable under the prevailing social opinion. See BW art.6:162. The Austrian ABGB system rests strictly on fault-based liability. See § 1295 Abs. 1 ABGB, translated in GENERAL CIVIL CODE OF AUSTRIA 253 (1972). See also WALTER VAN GERVEN ET AL., CASES, MATERIALS AND TEXT ON NATIONAL, SUPRANATIONAL AND INTERNATIONAL TORT LAW, 2-7 (Hart Publishing, 2000).

leading to the take down of content will he be held liable.

C. No General Obligation to Monitor

Article 15 of the Directive states that Member States shall not impose a general obligation on providers to monitor the information they transmit or store when they are performing one of the services analyzed above, namely mere conduit, caching, and hosting, and also cannot compel them to seek facts or circumstances indicating illegal activity.⁷⁴ Basically, a general obligation to monitor the information cannot be imposed on providers under the Directive. This is very reasonable since such an obligation could render it almost impossible to provide services in a realistic and commercial way, if providers were obliged to check and control all the information that flows through their networks.

In its second paragraph, Article 15 establishes a more specific obligation for ISPs.⁷⁵ The ISP is obliged "to promptly inform the competent public authorities of alleged illegal activities" or information provided by the ISP's customers, or to "communicate to the competent authorities," at the request of the authorities, information that enables the identification of those customers with whom the ISP has a storage agreement.⁷⁶

This paragraph imposes a duty of communication from the ISPs to the competent authorities in the case of suspected illegal activities. It is assumed that Member States, when implementing this provision, shall take into account the proper legal judicial guarantees in order to balance all the rights at stake, namely the investigative rights of the Member States' organizations, versus the privacy and freedom of speech rights of the recipients of the ISPs services.⁷⁷ For instance, in Spain, the proposal for the transposition of the January 18, 2001 Directive⁷⁸ in this area establishes that the ISPs, in relation with their content, have the following disclosure obligations:

- to communicate to the judicial or administrative competent authorities, when they have knowledge that the alleged illegal activity performed by the recipient of the

74. Directive, *supra* note 3, at art. 15.

75. See generally Rosa Julia-Barcelo & Kamiel J. Koelman, *Intermediary Liability in The E-Commerce Directive So Far So Good, But It's Not Enough*, 16 *COMPUTER L. & SECURITY REP.* 231 (2000) (draft), available at <http://www.ivir.nl/publications/e-commerce.html>.

76. Directive, *supra* note 3, at art. 15(2).

77. *Id.* at art. 16.

78. ANTEPROYECTO DE LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO [Directive on the Information Society and Electronic Commerce], draft of January 18, 2001 (Spain) [hereinafter Spanish E-Commerce Directive].

service; and

- to communicate to the judicial or administrative competent authorities, at their request, the information that allows for the identification of the recipient of the services.⁷⁹

In relation with the provisions of Article 15.2 of the Directive, the Spanish proposal provides that “the competent judicial authority can request to any ISPs to supervise or to keep all the data related to a determined Web site for a maximum of six months and to put it available to the authority.”⁸⁰

As is seen in this proposal, judicial authorities are called to act in order to protect the rights of all parties involved.⁸¹ However, the statutory approach in relation to the duty of communication established by Article 15.2 has not been adopted by all Member States.⁸²

VIII. DIRECTIVE LOOPHOLES

The EU Directive falls somewhat short in some areas, specifically, in the Directive’s coverage of the notice requirement and procedure for blocking content, freedom of expression, and unfair competition.⁸³ Many concerns arise through the automatic imposition of liability on ISPs for the removal of content, as well as liability for information tool services [hereinafter ITS]. Since the first of the two have been addressed above,⁸⁴ the focus in the latter portion of this Article now turns to ITS liability.

79. See Spanish E-Commerce Directive *supra* note 78, at art. 12.1. “Comunicar a las autoridades judiciales o administrativas competentes, en cuanto tengan conocimiento de ello, la actividad presuntamente ilícita realizada por el destinatario del servicio; comunicar a las autoridades judiciales o administrativas competentes, a solicitud de éstas, la información que les permita identificar a los destinatarios de los servicios.” *Id.*

80. *Id.*, art. 12(d). “La autoridad judicial competente podrá requerir a cualquier prestador de servicios que supervise, o que conserve, todos los datos relativos a un determinado sitio de Internet durante un período máximo de seis meses y que las ponga a su disposición.” *Id.*

81. See generally *id.*

82. See Jean-Francois Lerouge, *The Liability of Internet Service Providers Within the E-Commerce Directive* at <http://www.eclip.org/conference/1st/lerouge.pdf> (last visited January 5, 2003).

83. Compare DMCA, *supra* note 2, at § (g)(2), with Directive, *supra* note 3.

84. See Directive, *supra* note 3, at art. 7(2).

A. The Liability of Information Tool Services

The ITSs, which include "search engines," are one of the most important actors in the everyday development of the Internet.⁸⁵ They allow users to find information in a network that is exponentially increasing its number of pages on an annual basis. ITSs perform their activities in two ways. The first is the creation of databases with Web sites arranged by thematic, geographic, or some other criteria that facilitate users in finding the sought-after data. Through user-entered prompts, ITSs also display lists of Web pages with requested information. For example, a user entering a search string using the term "electronic commerce," is presented with a list of Web pages containing at least one of the two words. However, if you want to narrow your search only to "electronic commerce in Italy," then only Web pages with at least one of these three words will appear.⁸⁶ The list of Web pages consists of links⁸⁷ included in the "search result" page of the ITS.

The next question that must be addressed is whether it is reasonable to impose liability upon an ITS that links to Web pages containing unlawful material. Is it reasonable to expect an ITS to know or have some reason to believe that any of the millions of Web pages that normally appear on the "search results" Web page could include illegal material? Or, in other words, it is reasonable to impose a duty of care on ITSs in order to control all the material that they provide, in an indirect way, through the links they display? To answer these questions, it should be explained very briefly how an ITS typically works. The indexing and searching functions are normally performed either by robots or by human beings.⁸⁸ It is obvious that the former cannot distinguish by itself whether a Web page contains illegal material. On the other hand, it can be argued that a human being can do so quite easily. However, it must be kept

85. See *ACLU v. Reno*, 929 F. Supp. 824, 837 (E.D. Pa. 1996).

86. This is a very basic description which does not cover the many options available with such searches. For instance, adding the symbol "+" between the words will allow you to obtain web pages that contain the three words mentioned.

87. Created by a process called "linking," defined as: "a process by which a hypertext link is made from one web site to another, using a hypertext mark-up language (HTML) link achieved by an on-screen underline or click facility, taking a customer from that point on the business's web site to the third party site to which the link has been achieved." See Robert Bond, Legal Updates, *International Legal Issues of E-Commerce*, at http://www.faegre.com/articles/article_204.asp (last visited January 5, 2003) (an association of ISPs in Belgium signed an agreement with that Member's government on May 28, 1999, establishing a different regulatory approach).

88. See David Kramer & Jay Monahan, *Panel Discussion To Bot or Not To Bot: The Implications of Spidering*, 22 *HASTINGS COMM. & ENT. L.J.* 241, 242 (2000).

in mind that human indexers of Web content typically work in a similar fashion to persons who index huge paper-based libraries; they only have time to take a quick glance at the Web pages to determine into which category the pages should be indexed. Therefore, it may be impossible for even human indexers to determine in a few seconds whether a certain Web page is displaying illegal material.

In the U.S., the DMCA has incorporated a liability limitation for the ITS's acts of linking users to a site containing infringing material, as long as the following conditions are met:

- the provider must not have the requisite level of knowledge that the material is infringing if the provider has the right and ability to control the infringing activity, the provider must not receive a financial benefit directly attributable to the infringing activity; and
- upon receiving notification of claimed infringement, in the form of a proper notice, the provider must expeditiously take down or block access to the allegedly infringing material.⁸⁹

In light of the abovementioned considerations, it is possible to outline the basic principles of liability exemptions that should be granted to ITS. First, ITSs should not be held liable for merely providing a link to a site containing illegal material, whether it is the product of a human or robot indexing function. Real persons have insufficient time to discern the character nuances of Web pages, and programmers likewise do not have the time or resources to design automated robots to filter out all illegal content. The scope of liability exemptions must cover both human and robot search engines. Additionally, ITSs should only be held liable in the case where they are well aware of the illegal content of a Web site indexed on their Web pages. This "awareness" requirement should be satisfied by "proper and complete" notice given by interested parties to an ITS, in the same manner as required under the DMCA. With these main provisions, the legal uncertainty that ITSs currently face could be avoided, in so far as the possible outcome of a complaint filed against an ITS for providing links to illegal material would be avoided.

89. See 17 U.S.C. § 512 (2002).

IX. CONCLUSION

As is seen, the EU Directive has some loopholes that need to be closed. The most troublesome of which include, a lack of a "notice and takedown" procedure, which threatens freedom of expression; and the fact that the current regime may actually promote unfair competition in some situations. The lack of a notice and take down procedure causes the ISPs to become a sort of censorship body, in order to avoid liability when they opt to take down a Web page upon receipt of a claim regarding the content on that page. This threatens freedom of expression as long as customers are without protection against unfounded complaints. Unfair competition may be promoted in cases where companies engage in a form of commercial war in cyberspace, lobbying bad faith claims against their competitor's Web content.

As a recommendation, it is proposed that a notice and take down procedure modeled after the DMCA be established, including notice to specialized bodies within the Member States' administrative structures or professional organizations.⁹⁰ Regarding the second Achilles heel of the EU Directive, in order to have a complete protection for all the parties involved, a "put back procedure" should be initiated. Such a procedure should give the owners of disabled Web sites the chance to exercise a defense and at least stave off an unwarranted blocking or removal of their content. Finally, liability must be imposed upon persons who intentionally transmit false or unfounded notices which lead to the removal of a Web page content.

In conclusion, the EU Directive on E-Commerce has set up a fair mechanism to limit an ISP's liability. However, loopholes in that prescribed plan present an impracticable future, when considering current technical developments, evolving Internet industry practices, and the discrepancies of national treatments within the EU Member States. The DMCA has addressed the Directive's loopholes in a proper way, providing an incentive for companies to set up their business in the U.S., rather than in the EU. It is therefore regrettable that in such an important field as e-commerce, the Directive has not achieved the necessary level of legal certainty that would encourage economic operators in the EU to enhance the development of their internal market.

90. KAMIEL KOELMAN, *LIABILITY OF ONLINE SERVICE INTERMEDIARIES* 60 (Inst. for Information Law, Amsterdam, Aug 1997).